A Survey on Cloud Security, Challenges and Mitigation

Md. Alimuzzaman(1333098)
Department Of Computer Science and Technology
University Of Bedfordshire
Luton, United Kingdom
md.alimuzzaman@study.beds.ac.uk

***Abstract*- Cloud computing has emerged around the world, and the use of it has become popular very quickly in organizations. Cloud computing make available for use many advantages like accessibility of data and low cost. Security is a major issue in cloud computing environment, because customer's stores confidential information's with a cloud storage provider, but these providers are not trusted. Cloud security is becoming a major concern for organizations. This paper discusses the security issues, i.e. risks, attacks that arise in cloud computing. Overview state various attacks and their mitigation techniques.**

***Index Terms*—Cloud computing, IaaS, Paas, Saas, Security, Risks, Attacks, Data.**

I. Introduction

"Cloud computing is the most enticing technology due to its flexibility and cost efficiency. With the help of this technology, industries can remove the expensive computing infrastructure which based on IT services and solutions. There is a extensive scope of cloud computing as many of the organizations have adopted it. Use of cloud computing in organisations can increase the capacity and capabilities of the software by many folds. Despite such successes and benefits, there are some concerns that can hinder the perception of cloud computing as one of the new IT model. It is essential for every organisation realise the issues related to cloud computing security, which may be arise due to the old problems in a new settings , IT departments are such in a position to develop and deploy applications at the cost of governance ."

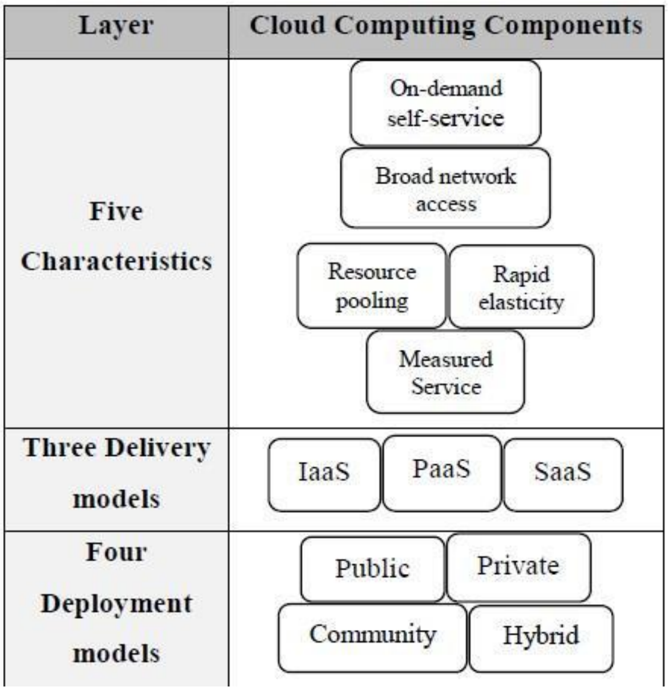
"There are some mixed issues and privacy challenges that are hardly needed to take care of for the security reasons of data centres are around any corner of the world, which are beyond the reach of the users. One of the major problems is server breakdown, this issue is witnessed at regular intervals, so it can be said that there are multifarious issues related to privacy and security in cloud computing. In this survey paper, the principles of cloud computing and its security will be explored, To provide a clear concept of security management, challenges, risks, threats, vulnerabilities, and ways to overcome those threats on cloud computing. This paper discusses about protecting the personal information from malicious persons."

II. Cloud Computing

"Cloud computing is a model that enables convenience in network access to configurable computing resources like networks, servers, applications, service, and storage, which can be released with minimal management efforts [1]. This model proposes cost saving benefits and increased IT agility. With the help of cloud computing, the network access techniques guarantee good service provider interaction with the user [2]."

III. Cloud Computing Components

"The cloud computing has various characteristics, deployment and delivery models. The five features are resource pooling, location independent, rapid elasticity, broad network access, on-demand self-service and measured service [3].These characteristics are shown in the figure below, which represents the first layer of the cloud environment architecture.



Layer	Cloud Computing Components
Five Characteristics	On-demand self-service Broad network access Resource pooling Rapid elasticity Measured Service
Three Delivery models	IaaS PaaS SaaS
Four Deployment models	Public Private Community Hybrid

Figure 1: Cloud structure [6]

The three models are **PaaS** (Platform as a service), **IaaS** (Infrastructure as a service), and **SaaS** (Software as a service). **IaaS** provides benefits to the user through data storage, computing services, and networking infrastructure. Delivery of computer infrastructure as a service is also well known as IaaS, for example, Amazon web service [4].

PaaS, through service provider's resources and the user can run custom applications or it can be explained as the process of computing platform and its solution as a service. Example is Google apps.

SaaS, it provides licensed application to the user to use running software on provider's infrastructure. Example is Salesforce.com CRM application [5]. The key model represents the second layer in the above diagram.

The other model is cloud deployment model, which includes public, private, community, and hybrid clouds and specially represents the third layer of cloud environment architecture. **Public cloud**, when public and multi tenants can access to the cloud environment is known as public cloud. **Private cloud**, the cloud which is accessible to a specified group and when the cloud is for a particular group is called as **community cloud**. **Hybrid cloud** can be defined as the form of two or more clouds like private and public or public and hybrid.

Kamara and Lauter[4] put more emphasis on two types of cloud i.e. private and public cloud. In a private cloud, the trusted users are owned and managed its infrastructure. But In public cloud ,it is controlled by cloud provider, which is not safe because the date shared with the untrusted servers.

IV. SECURITY RISKS

Cloud computing has its advantages, but there are certain risks associated with it, i.e. security risk, which play an important role in cloud computing environment [7]. Users who are using network facilities to share online data are well versed about the impending risk of loss of privacy [8].As per IDC survey, the major challenges related to cloud computing is security. It is very important to protect confidential and vital information of the user, as credit card details and patient's medical records from wicked users [9].

There are several challenges in moving the database to a large data centre; such security challenges can be virtualization vulnerability, privacy and control issues, accessibility issues, data loss or theft, integrity, and confidentiality. According to Amazon [10]the EC2 of Amazon addresses the security controls pertaining to physical, virtualization, and environmental security, whereas, for IT systems like operating systems, applications, and data, the users are still responsible for the security control.

"As per Tabaki et al. [3] The responsibility for privacy and security in cloud computing lies between the user and cloud service provider, but in delivery model the responsibility differs. As in SaaS, cloud providers are considered more accountable for securing the application services rather than the user. The public cloud environment has more responsibility as compared to other clouds because the client needs strict security. In PaaS, users are considered more responsible towards the application service that they build and run on the platform while the cloud providers are accountable for securing user's application from other users. In IaaS, the users protect the operating system and applications and the providers are responsible for protecting the user's data. "

According to [11] claim that IaaS has different security issues. The public cloud has a higher impact of security issues as compared to a private cloud. If there is any loss of physical infrastructure security issue or any failure cause by the management because of the management of infrastructure will be a great trouble. However, physical infrastructure is required for data processing and storage in the cloud environment, which can have a negative impact due to security risk. The transmitted data path can be affected to several third party infrastructure devices [11].

The cloud server which is built over the internet, so any issues to internet security will cause problem to the cloud services. Cloud data are transmitted through the internet, so if the provider highlight on cloud service security even then there would be a risks pertaining to the data transfer through network. It is evident that security problems on the internet will affect the cloud's valuable resources stored within the cloud. Encryption procedure and secure protocols are not a reliable source to defend data transmission over cloud, so to protect the data transmission by hackers and cybercriminals remedial steps need to be taken.

There are three security factors that affect the cloud, i.e. data integrity, data intrusion, and service availability.

A. Data integrity

The major security issue associated to cloud security risk is its data integrity. In the case of transition operations from or to the providers, the data stored may get effected. According to Cachin et al. [12]there are certain characteristics of risk of attacks from both outside and inside the cloud such as the red Hat Linux's distribution server [13]. The other example is of breached data in Google Docs in 2009, which started the Electronic Privacy Information Centre for the Federal Trade Commission to open an investigation into Google's cloud computing [12]. Another example of risk to data integrity was in Amazon S3, where the user suffered from data corruption [13].

Cachin et al. [12] argued that it was difficult to manage the data corruption, when many clients and devices are synchronized by a single user. Many researchers says that by using Byzantine fault-tolerant replication protocol within the cloud, the data corruption problem can be solved [14].However, Cachin et al.[12] claimed that it is not a appropriate method to explain the problem of data corruption because the servers belongs to cloud providers who use the same system installations and they located at the same place. Cachin et al. [12] says that even if the protocol solves the problem from cloud storage perspective, but the major problem lay at user's end. The cloud is most trusted among users because they trust cloud as a single reliable domain without the knowledge of the protection protocols. [12] Suggested that if Byzantine fault-tolerant protocols is beneficial used across multiple clouds from different providers.

B. Data Intrusion

Data intrusion is the other security risk associated with a cloud provider; there is an example of data intrusion, i.e. Amazon cloud service [6]. If someone can hack the account password of Amazon users, then the person can access all information's and the resources from the user's account. Thus, with a stolen password, a hacker can delete all information's from the virtual machine. If the user tries to modify the account or even disable the account services, then there is a possibility for the hacker to hack the email too. As Amazon allows to reset a lost password by email, so a hacker can also visit email to hack the new password. "

C. Service Availability

The other issue related to security risk is service availability. Amazon has clearly mentioned in their licensing agreement that there might be a situation of service unavailability time to time

[6]. It was earlier stated that if any user's file will break the cloud storage policy, then the user's web service will be terminated at any time. Moreover, if there would be any loss to Amazon web service and the service fails, the company is not going to pay any charge. "

If the company wants to secure the services from such failure, needs measures such as backups or use of multiple providers [6]. Recently, Google mail and Hotmail experienced service downtime. If there is any delay of the payment from the user for cloud storage then, the user may not be capable of getting access of their data. As a cloud storage provider, Linkup (Media Max) lost its 45 percent of stored client data [12].

According to [6] the privacy of information is not guaranteed in Amazon S3. The researcher claims that instead of using Amazon's advice of encrypting the data before storing them in Amazon S3, organizations should use HMAC technology or a digital signature [6]. By using these technologies, the user can ensure that the data is not modified by Amazon S3 and also protect the data moderation from hackers who have their stolen passwords or have access to their emails [15].

V. Security attacks and its alleviation in the cloud

There are several security concerns that prevent the misuse of cloud by customers. There are certain security threats, which discussed below, and their mitigation techniques are also explained on experience of implementation of cloud.

A.VM- Level attacks

Cloud computing is based on the same VM technology. In the implementation process of cloud, a hypervisor is used, i.e. VMware, vSphere, Xen, Microsoft virtual PC[16]. VM level threat appears due to the vulnerabilities in the hypervisor as the developers of this hypervisor have overlooked some facts while coding them.

Mitigation

The threat of VM level attack appears due to its vulnerabilities, but it can be alleviated by monitoring hypervisor through the IDS / IPS and the threat of VM attack can be mitigated by putting firewall.

B. Misuse of cloud computing

This type of threat arises due to the weak registration system in the cloud computing environment, as anyone can register themselves in the cloud computing registration process through a valid credit card and can use the service [17].This facilities the nefarious use of cloud computing, which brings ambiguity due to which attackers and malicious insiders can attack the system.

Mitigation

The threat of nefarious use of cloud computing can be alleviated in the ways mentioned below:

- Strict registration and validation process must be followed .
- The other way can be through monitoring and coordinating the credit card fraud.
- Before registration, proper and detailed introspection of the user's traffic network must be done.
- Organisations can block the network through monitoring public blacklist simply to avoid this type of threats. •

C. Doubtful interfaces and APIs

APIs or a set of software interfaces is used by consumers to interact with cloud services. These interfaces are used for management, provisioning, monitoring of the cloud services [18]. If these interfaces are weak, that can lead to several security threats like reusable tokens or passwords, anonymous access, clear text authentication, improper authorizations, limited monitoring, and logging capabilities.

Mitigation

The security model of cloud provider interfaces must be analyzed to mitigate the above-defined risks. To secure cloud computing, proper and strong authentication access controls must be implemented. The other way to reduce the risk is by encrypting the data, which is used in transmission and dependency chain related to API must be clearly understood. ”

D. Data loss or leakage

With data loss and leakages many organizations has to face brand deterioration and their reputation is at stake because the trust and morale of customer are eroded [19]. The loss of data or leakage which can be because of insufficient authentication, authorization and audit controls, disposal challenges, data centre reliability, disaster recovery, and inconsistent use of encryption and software keys. ”

Mitigation

This threat can be alleviated through encrypting ,protecting when the data is in transit; the protection of data at design and run time is opportune broke down, there must be a solid key era, stockpiling, and administration.

E. Loss of administration

While utilizing the cloud framework, the customer offers control to the cloud supplier on different issues. The SLA (Service level assent ion) may not be completely dedicated to the cloud supplier to give administrations. Along these lines, this crevice in security will prompt influencing the resistance security [20].

Mitigation

There are no such particular guidelines identified with distributed computing security, so it is essential for the association to put cautious endeavours for the execution of SLA (administration level assertion).

F. Lock-IN

Lock-IN is characterized as the powerlessness of the client to relocate one cloud administration supplier to an alternate. This risk happens due to the loss of versatility of client information and projects [21]. There are just few apparatuses, techniques or standard information groups, which give administration and information compactness. These circumstances keep clients or association from utilizing distributed computing.

Mitigation

To relieve Lock-IN danger, institutionalized cloud API (Application programming interface) ought to be utilized. This institutionalization gives acknowledgement to the distributed computing, which will build the quantity of cloud clients.

G. Segregation disappointment

In distributed computing, the administrations are conveyed by offering framework. The segments of distributed computing that are utilized to assemble circle parts, realistic transforming units, CPU store are not composed in a manner to give solid confinement properties [22].

The fundamental or primary building piece of distributed computing is hypervisor, which have uncovered the blemishes in working framework that empowers an unapproved control. With the assistance of disconnection disappointment, the assailants attempt to increase unapproved access to information of other cloud clients.

Mitigation

There must be solid compartmentalisation so that any individual can't hurt the operations of any cloud client. This danger can be moderated through actualizing best practices for arrangement, establishment, advancing confirmation and control, fixing the vulnerabilities and leading weakness checking, setup review, and observing the earth for unapproved changes.

H. Record seizing and administration commandeering

The dangers examined above was because of phishing, extortion, and programming vulnerabilities. The assailants or vindictive insiders can take the accreditations trough which they can get to the sent distributed computing administrations [23]. These dangers lead to trade off in secrecy, respectability, and accessibility of the administrations.

Mitigation

To alleviate the burglary danger of qualifications, the imparting of certifications between clients ought to be restricted, multi-component verification methods ought to be utilized. There ought to be strict checking to recognize the unapproved action and security approaches to stay away from record capturing.

I. Malicious insiders

Very nearly every association is knowledgeable with this danger as the effect of pernicious insider on associations is impressive. Vindictive insiders can invade associations and can harm brand name and resources of the organization [24]. They can likewise make monetary misfortune and benefit misfortune to an association. Thus, the clients of cloud administrations must realize that what controls can guard and secure their information from malevolent insiders.

Mitigation

By tagging the human asset prerequisites as a piece of lawful contracts or through leading, a thorough supplier evaluation can help in moderating this danger or assault. Malevolent insiders can likewise be ceased by giving straightforwardness into administration hones; general data security furthermore must focus the break notice forms.

J. Administration interface trade off

The administration interface of the cloud supplier is open through web. With the assistance of these interfaces, bigger set of assets can be gotten to [25]. Through client administration interface, clients can have remote access, which may present a danger or assault if the web program have a few vulnerabilities.

Mitigation

To alleviate the danger because of remote access, secure convention must be utilized to give access. On the off chance that cloud administration suppliers offer remote access to the clients, then they must fix all the vulnerabilities show in the interface.

K. Agreeability dangers

This assault or danger can emerge because of absence of administration over reviews and industry-standard appraisals. Because of absence of administration, clients of cloud administrations can't get a profound understanding about the methodologies, methods, and practices of the supplier in the region of access, character administration, and isolation of obligations.

The distributed computing administration suppliers may put associations at danger, who needs to acquire confirmation. Because of non accessibility of proof of their agreeability may not allow a review by cloud client.

Mitigation

To moderate the assault or dangers of consistence, the merchant's inward process ought to be explored. It should likewise be taken consideration that how often it is audited by external agencies or either it is open to being audited for compliance.

VI. Reliable cloud infrastructure

Cloud computing requires deployment of virtualization technologies. The organizations be likely to deploy their virtualization by using retrofitting the virtual network with the physical network. This situation occurs because of The network security teams not involved in the initial planning [20]. Due to the absence of technological awareness, network security weakens, and this is the cause cloud computing has a success in large organizations. The organizations can save themselves from all security threats and attacks by using the proper cloud security planning. There are some key points in the security architecture, and the points are discussed below:

A. Single Sign-On

Implementation of strong authentication is very difficult at the user level because, workers login to multiple applications and services. It is suggested that ,implement very strong authentication within the cloud and streamline the security management, organisations must implement Single Sign-On for cloud users. As single sign on enable a user to use multiple services and application in the cloud environment through a single login. It also provides a strong authentication at user level.

B. Increase Availability

The access to cloud service must be available all the time, even during maintenance, so that the critical data can be stored in the cloud that will be always available to the users. The faster availability of business data can help in reducing network downtime and can increase business profits [26]. The faster availability of data and increase access availability can be done through implementing technologies like dynamic server load balancing active clustering, and ISP load balancing within the network infrastructure.

C. Defense in Depth Approach

There must be proper layered defense consisting of intrusion detection, perimeter protection, and prevention components within the network [27]. To provide defense, virtual firewall appliances should be used instead of deploying the first generation firewalls. The virtual firewalls will allow network administration to inspect the traffic of all levels; that includes basic web browser traffic, encrypted web traffic and to peer-to- application traffic in the SSL tunnel. to protect networks from internal threats from insiders, IPS should be installed.

D. Single Management Console

The risk rises with the increased protective devices installed to safe the virtual network. Because of the human error involved, deployment of much more protection devices will gear up the management consoles also [28]. Therefore, to overcome the issue. There have to be a single management console to manage, configure and monitor all devices.

E. Virtual Machine safety

Virtual machines are used for every cloud implementation; these machines are vulnerable like their physical counterparts [29]. To protect the virtual machines, they must be inaccessible from other networks and deep check-up at the network level should have maintained so to protect them from threats which can be internal or external. Unauthorised access should be stopped by using IPS which prevents the intrusion, and unauthorized external access also keep safe by using some technologies, such as IPSec, SSL, VPN [30]. Based on the above study, protected cloud infrastructure is physically performed which has shown bellow in figure 2.

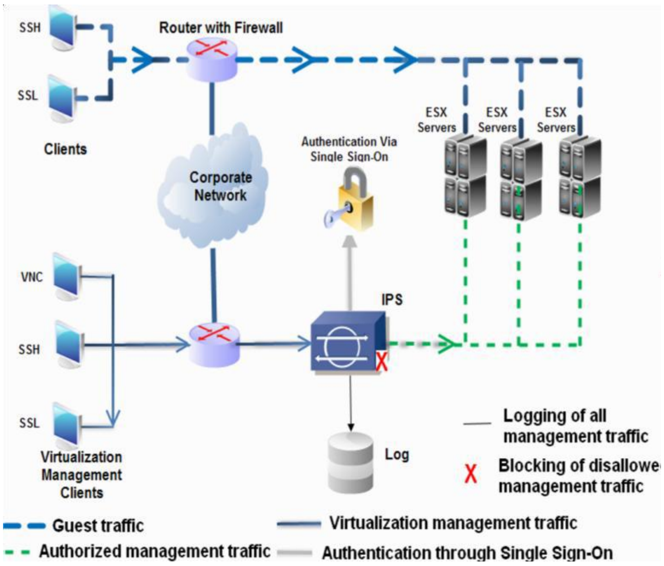

SSH
SSL
Clients
Router with Firewall
Corporate Network
Authentication Via Single Sign-On
ESX Servers
ESX Servers
ESX Servers
VNC
SSH
SSL
Virtualization Management Clients
IPS
Log
Logging of all management traffic
X Blocking of disallowe management traffic
Guest traffic
Authorized management traffic
Virtualization management traffic
Authentication through Single Sign-On

Figure 2: protected cloud infrastructure [20]

VII. Future Work

The main aim for the future work is to provide a safe cloud database, a structure to supply which will help to decrease the security risks faced by cloud computing. The architecture will have multi clouds, secret sharing of algorithm that will reduce the chance of the data intrusion, loss of service availability and also ensure the data integrity.

Regarding the loss of data, if the data is replicated in different cloud providers, then the risk can be reduced. As, if one cloud provider will fail, then the data can be accessed live through the other cloud provider. In future, more focus can be given to the cloud security architecture, through which various attacks and risks can be avoided.

VIII. Conclusion

It can be finished up from the above talk that, the utilization of distributed computing has quickly expanded, however security is still exceptionally real issue in the distributed computing environment. There are a few pernicious insiders who attempt to get to the client's record for their individual data, this lead to loss of information and clients has confronted issues identified with loss of administration accessibility. Notwithstanding, information interruption additionally prompts issues for the client in distributed computing. The clients likewise confront certain assaults on their cloud yet these assaults or dangers can be changed through a few systems like IPS (Intrusion Prevention System), detail human asset necessities to keep the cloud administration suppliers from vindictive insiders and a lot of people more relief methods are received to evade certain assaults and dangers. Associations that are actualizing distributed computing by growing the iron reason base ought to be mindful of the security assaults. To secure the consistence honesty and security of application and information, a protection line must be connected. Which will incorporates firewall, interruption discovery and counteractive action, uprightness and observing, login assessment, furthermore malware security. Endeavours must receive secure cloud structural engineering to keep away from specific dangers and assaults from interlopers. A physical distributed computing security construction modelling graph introduced. Later on, the proposed graph may be changed with cutting edge security advances utilized for executing the cloud security building design.

References

[1] NIST, [Online]. Available at: http://www.nist.gov/itl/cloud/[Accessed on 7 December 2014].

[2] P. Mell, T. Grance, “The NIST Definition of Cloud Computing,”. NIST Special Publication,2011,pp 850-857.

[3] H. Takabi et al."Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, vol. 8, no.6, 2010, pp. 24-31.

[4] S. Kamara and K. Lauter, "Cryptographic cloud storage", FC'10: Proc. 14thIntl.Conf. on Financial cryptograpy and data security, 2010, pp. 136-149.

[5] H.Takabi, J.B.D. Joshi and G.J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments", IEEE Security & Privacy, vol. 8, no.6, 2010, pp. 24-31.

[6] M.A. Alzain, E. Pardede, B. S, J. A. Thom. Cloud computing security: From single to multi clouds. IEEE computer society.

[7] J. Viega, "Cloud computing and the common man", Computer, vol.42, 2009, pp. 106-108.

[8] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, vol.40, 2009, pp. 81-86.

[9] H.Mei, J. Dawei, L. Guoliang and Z. Yuan,"Supporting Database Applications as a Service", ICDE'09: Proc. 25thIntl.Conf. on Data Engineering 2009, pp. 832-843.

[10] G. Brunette and R. Mogull, "Security guidance for critical areas of focus in cloud computing", CloudSecurityAlliance, 2009.

[11] T. Ristenpart, E. Tromer, H. Shacham and S. Savage, "Hey, you, get off of my cloud: exploringinformation leakage in third-partycompute clouds", CCS'09: Proc. 16thACM Conf. on Computer and communications security, 2009, pp. 199-212.

[12] C. Cachin, I. Keidar and A. Shraer, "Trusting the cloud", ACM SIGACT News, 40, 2009, pp. 81-86.

[13] .RedHat. [Online]. Available at: https://rhn.redhat.com/errata/RHSA2008-0855.html[Accessed on 7 December 2014].

[14] M. Vukolic,"The Byzantine empire in the intercloud", ACM SIGACT News, 41,2010, pp. 105-111

[15] Sun. [Online]. Available at: http://blogs.sun.com /gbrunett/entry/ amazon_S3_silent_data_corruption [Accessed on 7 December 2014].

[16] M. Jensen, J. Sehwenk et al., “On Technical Security, Issues in cloud Computing ”IEEE International conference on cloud Computing, 2009.

[17] B. R. Kandukuri, R. Paturi, A. Rakshit.Cloud Security Issues. 2009 IEEE International Conference on Services Computing. IEEE Computer Society.

[18] Z. Xuan, N. Wuwong , et al., "Information Security Risk Management Framework for the Cloud Computing Environments," in 2010 IEEE 10th International Conference on Computer and Information Technology (CIT), 2010, pp. 1328-1334.

[19] S. Chaves, C. Westphall and F. Lamin, "SLA Perspective in Security Management for Cloud Computing," in Sixth

International Conference Networking and Services, 2010, pp. 212-217.

[20] A. Celesti, F. Tusa, M. Villari and A. Puliafito, How to enhance Cloud architectures to enable cross-federation, CloudComputing (Cloud), 2010 IEEE 3rd International Conference on, Seiten 337 – 345, 2010.

[21] Z. Shen, Q. Tong. 2010. The security of cloud computing system enabled trusted computing technology. Signal Processing Systems (ICSPS), Dalian, 2010.pp. 11-15.

[22] Zhao, G., C. Rong, M. Jaatun, F. Sandnes, "Reference deployment models for eliminating user concerns on cloud security", The Journalof Supercomputing, 2010.

[23] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring data storage security in cloud computing", ARTCOM'10: Proc. Intl. Conf. on Advances in Recent Technologies in Communication and Computing, 2010, pp. 1-9.

[24] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, vol.34, no.1, 2011, pp 1-11.

[25] F. Schneider and L. Zhou, "Implementingtrustworthy services using replicated statemachines", IEEE Security and Privacy, vol.3, no.5,2010, pp. 151-167.

[26] Q. Liu, G. Wang, J. Wu, “Efficient Sharing of Secure Cloud Storage Services,” International Conference on Computer and Information Technology, 2010.

[27] Zhang Yaoxue and Zhou Yuezhi, "A New Cloud Operating System:Design and Implementation Based on Transparent Computing," Acta Electronica Sinica, Vo1.29,May.2011,pp.985- 990.

[28] A. Bhardwaj and V. Kumar, “Cloud security assessment and identity management,” in 2011 14th International Conference on Computer and Information Technology (ICCIT), 2011, pp. 387–392

[29] R. Neisse, D. Holling, and A. Pretschner, “Implementing Trust in Cloud Infrastructures,” in 2011 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid), 2011, pp. 524-533.

[30] K. Beaty, et al., “Network-level access control management for the cloud,” in Proc. 2013 IEEE Int. Conf. Cloud Eng.